

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

# MULTIMEDIA UNIVERSITY

## FINAL EXAMINATION

TRIMESTER 3, 2016/2017

### TAC3121 – APPLIED CRYPTOGRAPHY

(All Sections / Groups)

31<sup>st</sup> MAY 2017

2.30 p.m – 4.30 p.m

(2 Hours)

---

#### INSTRUCTIONS TO STUDENT

1. This Question paper consists of 3 pages with 5 Questions only.
2. Attempt **ALL** questions. All questions carry equal marks (12 marks) and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

**Question 1**

- 1a) Give the definition for the three aspects of information security, namely, security attack, security mechanism and security service. [3 marks]
- 1b) State the comparable key sizes for ECC, equivalent to 1024 and 2048 bits DSA? [2 marks]
- 1c) State the role of a compression function in a hash function? [3 marks]
- 1d) Using a diagram, describe DES Encryption. [4 marks]

**Question 2**

- 2a) Prove that  $(a \bmod n) \times (b \bmod n) = (a \times b) \bmod n$ . [2 marks]
- 2b) Use Euclidean algorithm to compute greatest common divisor (20, 50). [2 marks]
- 2c) If a character in plaintext is changed, how many character(s) in Playfair Cipher will be affected? [2 marks]
- 2d) Encrypt the plaintext "score a" using Hill Cipher with the key  $K = \begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$ . [6 marks]

**Question 3**

- 3a) Given the parameters of a Diffie-Hellman key exchange as  $q=353$ ,  $a=3$ ,  $X_A=60$ ,  $X_B=51$ . What is the value for the shared key  $K_{AB}$  and  $K_{BA}$ ? [5 marks]
- 3b) You are given the following information. Use RSA decryption to find M. [5 marks]  
  
 $C = 10; e = 5; n = 35;$
- 3c) Using the Rail Fence cipher of depth 2, decipher the following: [2 marks]  
  
WAEONOUCEERBRTSCED

Continued...

**Question 4**

- 4a) Cryptography can operate under Finite Fields only and it cannot operate under non-Finite Fields. Explain the reason behind this? **[3 marks]**
- 4b) Do you agree that the substitution cipher is more secure than the transposition cipher? Justify your answer. **[3 marks]**
- 4c) Diffie-Hellman Key Exchange is vulnerable to man-in-the-middle attack. Suggest a solution for this attack. **[3 marks]**
- 4d) Is it necessary to recover the secret key in order to attack a message authentication code (MAC) algorithm? Explain your answer. **[3 marks]**

**Question 5**

- 5a) Compare message authentication code (MAC) and Hash function. **[4 marks]**
- 5b) Symmetric cryptography is used in Key Management. Explain how it is used. **[4 marks]**
- 5c) Explain any **FOUR** requirements that a digital signature scheme must satisfy. **[4 marks]**

**End of Page**